Discrete Mathematics 61 (1986) 151–164
North-Holland

CYCLIC CODES OVER GF(q) WITH SIMPLE ORBIT STRUCTURE

W. Edwin CLARK
Department of Mathematics, University of South Florida, Tampa, FL 33620, U.S.A.

Received 19 October 1984
Revised 25 September 1985

Let C be a cyclic (n, k) code over $F = \mathrm{GF}(q)$ with generator polynomial $g(x)$ and parity check polynomial $h(x) = (x^n - 1)/g(x)$. Let G denote the subgroup of the group of units of the algebra $F[x]/(x^n - 1)$ generated by $x + (x^n - 1)$ and the nonzero elements of F. This group acts on C by left multiplication and the elements in an orbit have the same weight. We say that C has *simple orbit structure* if the generators of C form a single G-orbit. This implies that the set of generators of each ideal in C is also a single G-orbit which makes it possible to determine the weight distribution of such a code with relative ease. The main result of this paper is the determination of all polynomials $h(x)$ for which C has simple orbit structure. The proof proceeds by reducing the problem to a study of the group of units of the 'parity check' algebra $F[x]/(h(x))$.

1. Preliminaries

Let C denote a cyclic (n, k) code over $F = \mathrm{GF}(q)$ with parity check polynomial $h(x)$ and generator polynomial $g(x)$ of degrees k and $n - k$, respectively. We assume always that $n = \exp(h(x))$, i.e., n is the multiplicative order of x modulo $h(x)$. This merely rules out codes that are repetitions of smaller codes.

Definitions

$R = F[x]/(h(x))$, the parity check algebra of C,

$R^* =$ the group of units of R,

$\langle x \rangle =$ the subgroup of R^* generated by $x + (h(x))$,

$G = F^*\langle x \rangle$, where $F^* = F - \{0\}$,

$\mathrm{index}\langle x \rangle =$ the index of $\langle x \rangle$ in R^*.

Since we assume $n = \exp(h(x))$, x has the same order modulo $h(x)$ as it does modulo $x^n - 1$. So the group G may be assumed (by appropriate identification) to act on both C and R by left multiplication. These group actions are isomorphic via

$$f(x) + (h(x)) \mapsto f(x)g(x) + (x^n - 1).$$

(This mapping is not an algebra isomorphism. However R and C are isomorphic as algebras if (and only if) $h(x)$ and $g(x)$ are relatively prime; this is the case under the common assumption $(n, q) = 1$. We do not require this here.)

Since C is cyclic, elements in the same G-orbit have the same weight. We are interested in the orbit structure of G acting on C which as noted above is the same as that of G acting on R. We show how to define the weight of an element of R without reference to C so that corresponding elements of R and C have the same weight: Define $w_{h(x)}(f(x))$ to be the number of positive integers i no greater than n such that $x^i f(x) \pmod{h(x)}$ has degree precisely $k-1$. As noted in [1] this is equal to the weight of $f(x)g(x) + (x^n - 1)$ considered as an element of the code C.

For terminological convenience we often identify the code C, the polynomial $h(x)$ and the algebra R. (Note however that the algebra R does not uniquely determine the code C; rather, R together with a unit x that generates R as an algebra over F determines C.) So, for example, we say that $h(x)$ is *equidistant* if the code C is equidistant.

Definition. We say that $h(x)$ has *simple orbit structure* if $R^* = G$.

Note that the generators of the ideal C correspond to the units of R. So C has simple orbit structure means that the generators of C form a single G-orbit. We shall see that this implies that the generators of each ideal contained in C also form a single G-orbit.

Let us say that $h(x)$ is *local* if R is a local ring. Thus $h(x)$ is local if and only if $h(x)$ is a power of an irreducible polynomial. We will prove that $h(x)$ is local and has simple orbit structure if and only if $h(x)$ is one of the following three types of polynomials:

Type 1. $h(x)$ is a type I(a, k) polynomial over F if $F = \mathrm{GF}(q)$ and $h(x)$ is irreducible of degree k with exponent $(q^k - 1)/a$, where a divides $q-1$ and $(k, a) = 1$ $(\Leftrightarrow((q^k - 1)/(q-1), a) = 1)$. Note that $h(x) = x$ is not allowed since x is a unit modulo $h(x)$.

Type 2. $h(x)$ is a type II(a, b) polynomial over F if $F = \mathrm{GF}(p)$, where p is prime and $h(x) = (x-b)^2$, where b is a nonzero element of F of multiplicative order $(p-1)/a$. It follows that $h(x)$ has exponent $p(p-1)/a$.

Type 3. $h(x)$ is a type III polynomial over F if $F = \mathrm{GF}(2)$ and $h(x) = (x+1)^3$

We shall show that if a polynomial $h(x)$ over $F = \mathrm{GF}(q)$ has simple orbit structure but is not local then one of the following holds:

(i) $q = 2$ and $h(x)$ is a product of any number of local polynomials with simple orbit structure at most one of which is not of type I. (See Theorem 3 for necessary and sufficient conditions on the factors.)

(ii) $q = p$, an odd prime, and $h(x)$ is a product of two local polynomials of

which either both are type I or one is of type I and the other is of type II. (See Theorems 4 and 5 for sufficient conditions on the factors.)

(iii) q is any prime power and $h(x)$ is a product of two type I polynomials (See Theorem 4 for sufficient conditions on the factors.)

The following lemma is crucial in all that follows.

Lemma 1. *Let* $h(x) = h_1(x)h_2(x)$, $n = \exp(h(x))$ *and* $n_1 = \exp(h_1(x))$. *Then*

$$w_{h(x)}(c(x)h_2(x)) = (n/n_1)w_{h_1(x)}(c(x)). \tag{1}$$

Proof. One easily checks that

$$c(x) \pmod{h_1(x)} = (c(x)h_2(x) \pmod{h(x)})/h_2(x). \tag{2}$$

The left side of Eq. (1) is the number of terms in the sequence

$$x^i c(x)h_2(x) \pmod{h(x)}, \quad i = 1, 2, \ldots, n$$

of degree exactly $k-1$. Dividing each term of this sequence by $h_2(x)$ and using Eq. (2) we see that this is the same as the number of terms in the sequence

$$x^i c(x) \pmod{h_1(x)}, \quad i = 1, 2, \ldots, n$$

of degree exactly degree $(h_1(x)) - 1$. This latter sequence is however an n/n_1-fold repetition of the first n_1 terms since n_1 is the order of x modulo $h_1(x)$. This establishes Eq. (1). □

Corollary 1. *Every divisor of an equidistant polynomial is equidistant.*

2. Equidistant cyclic codes over GF(q)

In [1] we stated the following theorem.

Theorem 1. *A polynomial is equidistant if and only if it is a type* I *polynomial.*

Proof. A proof was given in [1]. However there is an error in the proof of statement (3) on page 140 of that paper where it was inadvertently assumed that the nonunits of R form an ideal. This is equivalent to assuming that $h(x)$ is local. We fill this gap by establishing the following.

Proposition 1. *If a polynomial is not local, then it is not equidistant.*

Proof. We assume the result actually proved in [1] that a local polynomial is equidistant if and only if it is what we call in this paper a type I polynomial. Using this together with Corollary 1, if there is a non-local equidistant polynomial then

there is an equidistant polynomial $h(x)$ which is a product of two type I polynomials $h_i(x)$, $i=1, 2$, with exponents $n_i=(q^{k_i}-1)/a_i$, where a_i divides $q-1$. The exponent n of $h(x)$ is $[n_1, n_2]$ and the degree k of $h(x)$ is the sum of the degrees k_1 and k_2 of the two factors.

Now if $h(x)$ were equidistant the average weight

$$nq^{k-1}(q-1)/(q^k-1)$$

of the non-zero code words would be an integer and hence

$$D=n(q-1)/(q^k-1)$$

would also be an integer. We show that this is not the case. Observe that

$$q^k-1>(q^{k_1}-1)(q^{k_2}-1)=A.$$

This implies that the positive number $N=A/(q^k-1)$ is less than 1. On the other hand each n_i divides $M=A/(q-1)$. Therefore their least common multiple n divides M. In particular n is less than or equal to M. This implies that D is at most $M(q-1)/(q^k-1)=N<1$, a contradiction. This proves the proposition and establishes Theorem 1. □□

3. Determination of those $h(x)$ with simple orbit structure

Lemma 2. *If $k(x)$ divides $h(x)$ and $h(x)$ has simple orbit structure, then so does $k(x)$.*

Proof. Let R be the parity check algebra of $h(x)$ and let S denote the parity check algebra of $k(x)$. The natural mapping $\#: R \to S: f(x)+(h(x)) \mapsto f(x)+(k(x))$ is a surjective algebra homomorphism. It follows (see [3, p. 400]) that $\#$ restricted to R^* is a group homomorphism onto S^*. Since $\#$ clearly takes scalars to scalars and $x+(h(x))$ to $x+(k(x))$ we have $S^*=\#(R^*)=\#(\langle x\rangle)\#(F^*)=\langle x\rangle F^*$, as desired. □

We wish to determine all $h(x)$ with simple orbit structure. In general $h(x)$ is a product of local polynomials, which by Lemma 2 also have simple orbit structure. We begin with the local case.

Theorem 2. *A local polynomial has simple orbit structure if and only if it is a polynomial of type* I, II *or* III.

Proof. Let $F=\mathrm{GF}(q)$, where $q=p^s$ for a prime p. Let $h(x)=p(x)^t$, where $p(x)$ is a monic, irreducible polynomial over F of degree k. Thus $h(x)$ has degree kt.

We first assume that $R^*=G$ and show that this implies that $h(x)$ is one of the three types. If $t=1$, then $h(x)$ is irreducible and R is therefore a field. In this case

the non-zero elements of R are in fact the units of R and so $h(x)$ is equidistant. Hence from Theorem 1 we have that $h(x)$ has type I. We now assume that $t > 1$.

Let $|X|$ denote the number of elements in X. We first establish

$$|R^*| = (q^k - 1)q^{k(t-1)}. \tag{3}$$

Proof of Eq. (3). Since $h(x)$ has degree kt, R has dimension kt over F and so $|R| = q^{kt}$. On the other hand R is a local ring with maximal ideal $M = (p(x))/(h(x))$ and R/M is a field with q^k elements. It follows that $|M| = q^{kt-k}$. Since R is local, R^* is just the complement of M in R and so $|R^*| = |R| - |M|$, from which (3) follows.

$$|\langle x\rangle| = p^l \exp(p(x)), \quad \text{where } p^{l-1} < t \leqslant p^l. \tag{4}$$

Proof of Eq. (4). $|\langle x\rangle|$ is the order of x modulo $h(x) = p(x)^t$, i.e., the exponent of $h(x)$. Thus the result follows from [2, Section 6.2, pp. 150–151]. Note that what we call exponent here is called 'period' in [2].

$$\exp(p(x)) = (q^k - 1)/a, \quad a \mid q - 1 \quad \text{and} \quad (a, k) = 1. \tag{5}$$

Proof of Eq. (5). By Lemma 2 we have that $p(x)$ has simple orbit structure. As above for the case $t = 1$ it follows that $p(x)$ is equidistant and so, by Theorem 1, (5) holds, i.e., $p(x)$ is of Type I(a, k).

$$ap^{s(kt-k-1)} < p^l. \tag{6}$$

Proof of Eq. (6). Since $R^* = \langle x\rangle F^*$, index $\langle x\rangle < q$. That is, $|R^*|/|\langle x\rangle| < q$. Substituting the values from Eqs. (3), (4), and (5) we get (6).

$$l = 1 \quad \text{or} \quad l = 2. \tag{7}$$

Proof of (7). First note that from (6) we obtain

$$s(kt - k - 1) < l. \tag{8}$$

Since $k > 0$ this implies

$$s(t - 2) < l. \tag{9}$$

By Eq. (4): $p^{l-1} < t$, so

$$s(p^{l-1} - 2) < l. \tag{10}$$

Now if $l > 3$, by induction $l < p^{l-1} - 2 \leqslant s(p^{l-1} - 2)$ which contradicts (10).

Suppose $l = 3$, then by (4) we have

$$p^2 < t \leqslant p^3. \tag{11}$$

This implies that $4 < t$ and so $3 < t - 1$. Applying this to (8) we have

$$2 < s(k(t - 1) - 1) < l = 3.$$

This contradiction shows that l is not 3. So (7) is established.

$$\text{If } l=1, \quad \text{then} \quad k=1, s=1 \quad \text{and} \quad t=2. \tag{12}$$

Hence $h(x)=(x-b)^2$, where b is a nonzero element of GF(p), i.e., $h(x)$ is a type II polynomial.

Proof of (12). If $l=1$ we obtain from (8):

$$s(k(t-1)-1)<1. \tag{13}$$

Since we are now only considering the case $t>1$, (13) yields $s(k-1)<1$ which implies that $k=1$. Putting $k=1$ in (13) yields $s(t-2)<1$ and so we must have $t=2$. This means that $h(x)=(x-b)^2$, where $\exp(x-b)=$ the order of b in $F=\mathrm{GF}(p^s)$ has order $(p^s-1)/a$.

Now $(x-b)^2=x^2-2bx+b^2$ so in the ring R we have $x^2=2bx-b^2$ and by induction $x^i=ib^{i-1}x-(i-1)b^i$. From this we see that the smallest value of i such that x^i lies in F^* is p and $x^p=b^p$. It follows that $F^*\cap\langle x\rangle=\langle b^p\rangle$. Since $(p,(p^s-1)/a)=1$, $\langle b\rangle=\langle b^p\rangle$. It follows that $\langle x\rangle$ contains $(p^s-1)/a$ elements of F^*. So there are a $\langle x\rangle$-orbits that contain scalars. On the other hand the index of $\langle x\rangle$ in R^* is $q(q-1)/p(p^s-1)/a=p^{s-1}a$. So there will be enough $\langle x\rangle$-orbits containing scalars to cover R^* if and only if $s=1$.

$$\text{If } l=2, \text{ then } t=3, k=s=1 \quad \text{and} \quad p=2. \tag{14}$$

Hence $h(x)=(x+1)^3$, i.e., $h(x)$ is type III.

Proof of (14). From (4) we have

$$p<t\leqslant p^2$$

and so $2<t$. From (8) we have

$$s(k(t-1)-1)<2. \tag{15}$$

If $3<t$, then $2<t-1$ which conflicts with (15). If $t=3$, then (15) implies that $s(2k-1)<2$ which is only possible if $s=k=1$. Since $p<t$ and $t=3$, we must have $p=2$.

This completes the proof that if $h(x)$ has simple orbit structure then it is of type I, II or III. It remains to check that each of these three types have simple orbit structure. For type I see [1, p. 141]. For type II see the proof of (12) above. In the case of type III there is only a single polynomial over GF(2) which is easily checked. This completes the proof of Theorem 2. □

Remark. It is of interest to note that the algebras $R=F[x]/(h(x))$, where $h(x)$ is of type I, II, or III are precisely the finite local algebras such that R^* is cyclic (see Gilmer [4]). Note however that we are not just interested in the algebra R but in the particular representation of R determined by $h(x)$. We see below that for

non-local rings, being of simple orbit structure does not imply that the group of units is cyclic.

We now consider the general case

$$h(x) = h_1(x)h_2(x)\cdots h_s(x), \tag{16}$$

where the factors $h_i(x)$ are local and pairwise relatively prime. Letting $R_i = F[x]/(h_i(x))$ we have the algebra isomorphism

$$R \to R_1 \times R_2 \times \cdots \times R_s \tag{17}$$

given by the mapping

$$f(x) + (h(x)) \mapsto (f(x + (h_1(x)), \ldots, f(x) + (h_s(x))) \tag{18}$$

which, abusing notation, we may write as

$$f(x) \mapsto (f(x), f(x), \ldots, f(x)). \tag{19}$$

In particular we have

$$x \mapsto (x, x, \ldots, x)$$

and for a in F

$$a \mapsto (a, a, \ldots, a).$$

We use (18) or (19) to identify R with the product $R_1 \times \cdots \times R_s$.

If $n = \exp(h(x)) = |\langle x \rangle|$ and $n_i = \exp(h_i(x))$, then the above isomorphism yields

$$n = [n_1, n_2, \ldots, n_s], \tag{20}$$

where the brackets denote the least common multiple.

Restricted to the group of units of R the above isomorphism yields a group isomorphism:

$$R^* \to R_1^* \times \cdots \times R_s^* \tag{21}$$

and hence $|R^*| = |R_1^*| \cdots |R_s^*|$

If $h(x)$ has simple orbit structure we deduce immediately from Lemma 2 and Theorem 2 that each factor $h_1(x)$ in (16) is of type I, II, or III. But, not all such products have simple orbit structure.

Before continuing we collect here some information (see Table 1) on the three

Table 1

Polynomial type	$\lvert R\rvert$	$\lvert R^*\rvert$	$\lvert\langle x\rangle\rvert$
I(a, k)	q^k	q^{k-1}	$(q^k-1)/a$
II(a, b)	p^2	$p(p-1)$	$p(p-1)/a$
III	8	4	4

types of rings that we need below. (See the proof of Theorem 2 for the derivations.)

Theorem 3. *Let $F = \mathrm{GF}(2)$. Then $h(x)$ has simple orbit structure if and only if one of the following holds:*

(i) *$h(x)$ is a product of any number of primitive polynomials of pairwise relatively prime degrees.*

(ii) *$h(x)$ is a product of any number of primitive polynomials of pairwise relatively prime degrees and a single polynomial of the form $(x+1)^t$, where $t = 2$ or $t = 3$.*

Proof. Assume that $h(x)$ has simple orbit structure. Since F is the two element field this reduces to $R^* = \langle x \rangle$. Let $h(x)$ be as in (16). As pointed out, we know that each factor in (16) is one of the three types I, II, or III. In this case each of the factor rings R_i of (17) has a cyclic group of units. Since R^* is the product of these cyclic groups and is itself cyclic, the orders of the cyclic factors must be pairwise relatively prime. Conversely, using again the isomorphism (17), if the orders of the cyclic factors are pairwise relatively prime then $R^* = \langle x \rangle$.

If $q = 2$ and a polynomial is of type I(a, k), then $|R^*| = 2^k - 1$, but in the case of type II, or type III, $|R|$ is even. Note also that $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$. It follows that (i) or (ii) holds if and only if $h(x)$ has simple orbit structure. □

Note that for $h(x)$ to have simple orbit structure we must have at most $q-1$ orbits of $\langle x \rangle$ in R^*. This implies that index $\langle x \rangle$ is at most $q-1$. This is a necessary but not sufficient condition for $h(x)$ to have simple orbit structure. Nevertheless this condiution limits strongly the possibilities.

Lemma 3. *Let $F = \mathrm{GF}(q)$, where $q > 2$. Assume that $h(x)$ is a product of $s > 1$ polynomials $h_i(x)$ of types* I(a_i, k_i). *Then* index$\langle x \rangle \leqslant q - 1$ *if and only if*

$$s = 2, \qquad (k_1, k_2) = (a_1, a_2) = 1, \tag{21.1}$$

in which case $\langle x \rangle$ has index precisely $q-1$.

Proof. Since each n_i divides $q^{k_i} - 1$ we have from (20) that $n = |\langle x \rangle|$ divides the number

$$N = (q^{k_1} - 1) \cdots (q^{k_s} - 1)/(q-1)^{s-1}.$$

Hence $|\langle x \rangle| \leqslant N$. Since the R_i are all fields we have

$$|R^*| = N(q-1)^{s-1}$$

and it follows that the index$\langle x \rangle \geqslant (q-1)^{s-1}$. Assuming $R^* = F^*\langle x \rangle$, index$\langle x \rangle$ is at most $q-1$. Hence $s = 2$ and the index is precisely $q-1$.

Suppose that $s = 2$ and index$\langle x \rangle = q - 1$. Then $n = [n_1, n_2] = n_1 n_2/(n_1, n_2)$ and

$|R^*| = n_1 a_1 n_2 a_2$. So the index of $\langle x \rangle$ is $a_1 a_2 (n_1, n_2)$. Let $d = (k_1 - 1, k_2 - 1)$ and $a = [a_1, a_2] = a_1 a_2/(a_1, a_2)$. Now $(q^{k_1} - 1, q^{k_2} - 1) = q^d - 1$ and each a_i divides $q^d - 1$ so a divides $q^d - 1$. It follows that (n_1, n_2) is divisible by $(q^d - 1)/a$ and so the index of $\langle x \rangle$ is divisible by $(q^d - 1)(a_1, a_2)$. This implies that $d = 1$ and $(a_1, a_2) = 1$.

Conversely, if $s = 2$ and (21.1) holds, then using the conditions given in the definition of type I(a_i, k_i) polynomials one may verify that index$\langle x \rangle = q - 1$. □

Lemma 4. *Let* $F = \mathrm{GF}(p)$, *where* p *is an odd prime. If* $h(x)$ *has simple orbit structure then only two nonlocal cases are possible.*

(i) $h(x)$ *is a product of two polynomials, one of type* II(a_1, b) *and one of type* I(a_2, k), *where* $(a_1, a_2) = 1$. *In this case* index$\langle x \rangle = p - 1$.

(ii) $h(x)$ *is a product of two polynomials, both of type* I *and the condition* (21.1) *of Lemma* 3 *must hold.*

Proof. In this case we may assume that $h(x)$ is a product of polynomials of types I and II. If all are of type I, then (ii) holds by Lemma 3. By Lemma 2 we are left with just one polynomial of each type if we can rule out the two cases:

Case 1. $h(x)$ is a product of two type II polynomials with parameters (a_i, b_i), $i = 1, 2$.

Case 2. $h(x)$ is a product of two type I polynomials and one type II polynomial.

Suppose Case 1 holds. Then $n_i = p(p-1)/a_i$ and $|R_i^*| = p(p-1) = n_i a_i$. Hence $|R^*| = n_1 a_1 n_2 a_2$. Then $|\langle x \rangle| = [n_1, n_2] = n_1 n_2/(n_1, n_2)$. It follows that index$\langle x \rangle$ is $a_1 a_2 (n_1, n_2)$, which is divisible by $a_1 a_2 p$ which is greater than $p - 1$.

Suppose Case 2 holds. In this case $n = |\langle x \rangle|$ is the l.c.m. of $\exp(x - b)^2 = p(p-1)/a$ and $\exp(h_1(x)h_2(x)) = (p^{k_1} - 1)(p^{k_2} - 1)/(p - 1)$ by Lemma 3. It follows that n divides and is therefore $\leqslant p(p^{k_1} - 1)(p^{k_2} - 1)/(p - 1)$. Now $|R^*| = p(p-1)(p^{k_1} - 1)(p^{k_2} - 1)$ and hence index$\langle x \rangle \geqslant (p-1)^2$ which is greater than $p - 1$. This shows that Case 2 is impossible.

It remains to show that if $s = 2$, one factor is type II(a_1, b) and the other is type I(a_2, k), then $(a_1, a_2) = 1$ and index$\langle x \rangle = p - 1$. To see this note that $|R^*| = p(p-1)(p^k - 1)$ and n is the l.c.m. of $n_1 = p(p-1)/a_1$ and $n_2 = (p^k - 1)/a_2$. It follows that index$\langle x \rangle = a_1 a_2 (n_1, n_2)$ is divisible by $(a_1, a_2)(p - 1)$ which is greater than $p - 1$ unless $(a_1, a_2) = 1$ in which case the index is precisely $p - 1$. □

Lemma 5. *Let* $F = \mathrm{GF}(q)$, *where* $q > 2$ *and let* $h(x)$ *be a nonlocal polynomial satisfying the conditions of Lemma* 3 *or Lemma* 4. *Then* $h(x)$ *has simple orbit structure if and only if* $F^* \cap \langle x \rangle = \{1\}$.

Proof. This follows from the fact that in each of the lemmas $\langle x \rangle$ has index exactly $|F^*|$. □

Theorem 4. *Let $h(x) = h_1(x)h_2(x)$, where $h_i(x)$ is of type $\mathrm{I}(a_i, k_i)$ and $(k_1, k_2) = (a_1, a_2) = 1$. Then $h(x)$ has simple orbit structure if the following condition holds.*

$$\begin{aligned} &\textit{Every prime factor of } q-1 \textit{ divides either} \\ &(q^{k_1}-1)a_2/(q-1) \quad \text{or} \quad (q^{k_2}-1)a_1/(q-1). \end{aligned} \tag{22}$$

Proof. Use the identification $R = R_1 \times R_2$ given by (19), but write $x = (z, w)$ instead of (x, x) to avoid confusion. By Lemma 5 we must show that the only element of F in $\langle x \rangle$ is $1 = (1, 1)$. Suppose to the contrary that $x^i = (z^i, w^i) = (a, a)$ where a is a nonzero element of F of order $d > 1$. By Lemma 3, x has order $n = (q^{k_1}-1)(q^{k_2}-1)/(q-1)$. It follows that $i = (n/d)u$, where $(u, d) = 1$. By (22) we may assume that $(s, d) > 1$, where $s = u(q^{k_1}-1)a_2/(q-1)$. Let $c = w^{o(w)/d}$, where $o(w) = (q^{k_2}-1)/a_2$ is the order of w. Now c has order d and c^s has order d only if $(s, d) = 1$ which is not the case. Hence $a = w^i = c^s$ does not have order d. This contradiction proves the theorem. □

Corollary. *If $q = a_1a_2$, in particular, if $a_1 = q-1$ and $a_2 = 1$, then (22) holds.*

Remark. If (22) fails, $h(x) = h_1(x)h_2(x)$, where each factor is of type I, and (21.1) holds, then $h(x)$ may or may not be of simple orbit structure as we now show by example. It will follow that necessary and sufficient conditions that $h(x)$ be of simple orbit structure cannot be obtained in terms of q, k_i and a_i. However Lemma 5 does provide a n.a.s.c. in conjunction with Lemmas 3 and 4.

Example. Let $q = 8$ and let $F = \mathrm{GF}(q)$. Let F' and F'' denote extension fields of F of orders $q^2 = 64$ and $q^3 = 512$ and with primitive elements c' and c'', respectively. $R = F' \times F''$ and write $c = (c', c'')$. We note that $o(c') = 63 = 9 \cdot 7$, $o(c'') = 511 = 7 \cdot 73$, and hence $o(c) = 9 \cdot 7 \cdot 73$. We identify a in F with (a, a) in R.

Let $\langle c \rangle$ be the subgroup of R^* generated by c. We show that depending on the choice of primitive elements c' and c'' we can have either

$$|\langle c \rangle \cap F| = 1 \tag{23}$$

or

$$|\langle c \rangle \cap F| > 1. \tag{24}$$

We do this by first showing that (24) holds if and only if c^m lies in F where $m = o(c)/7$. Assume first that c^m is in F. Since c^m has order 7, all nonzero elements of F are in $\langle c \rangle$, so (24) holds. Assume that $c^m = (e, f)$ is not in F, that is, e is not equal to f. By the above listed orders for c' and c'' it is clear that both e and f have order 7. Suppose $c^i = (g, g)$, where g is not 1. Then c^i has order 7 and so $i = mu$, where $(u, 7) = 1$. Hence $e^u = f^u$ and since u is invertible modulo 7 this implies that $e = f$, a contradiction. Therefore (23) holds.

Now suppose that $c^m = (e, f)$, where $e \neq f$. Then $e = f^i$ for some $i \leq 6$ and for each i, $(c'')^i$ is a generator for F'' since $(i, o(c'')) = 1$. Now replacing c'' by $(c'')^i$ we get $c^m = (e, e)$. On the other hand if $c^m = (e, e)$, then we can choose another i so that $e^i = f$ is different from e. As before replacing c'' by $(c'')^i$ will yield $c^m = (e, f)$.

Now let $h(x) = h_1(x)h_2(x)$, where $h_1(x)$ is the minimal polynomial of c' and $h_2(x)$ is the minimal polynomial of c''. It follows from the isomorphism (19) and Lemma 5 that $h(x)$ has simple orbit structure or not depending on whether (23) or (24) holds.

Theorem 5. *Let* $F = \mathrm{GF}(p)$, *where* p *is an odd prime. Let* $h(x) = h_1(x)h_2(x)$, *where the first factor is type* $\mathrm{II}(a_1, b)$, *and the second factor is type* $\mathrm{I}(a_2, k)$ *and* $(a_1, a_2) = 1$. *Then* $h(x)$ *has simple orbit structure if the following holds.*

Every prime divisor of $p - 1$ *divides either* $(p^k - 1)a_1/(p - 1)$ *or* a_2. (25)

Proof. By Lemma 4: $|\langle x \rangle| = p(p^k - 1)$. In the notation of the proof of Theorem 4 $o(z) = p(p - 1)/a_1$ and $o(w) = (p^k - 1)/a_2$. The theorem now follows from the argument in the proof of Theorem 4. □

Corollary. *If* $a_1 a_2 = p - 1$, *in particular, if* $a_1 = p - 1$ *and* $a_2 = 1$, *then* (25) *holds.*

4. Weight distributions

We show how to compute the weight distribution for a cyclic (n, k) code with simple orbit structure. Let $h(x)$ be the parity check polynomial and let $f_1(x), \ldots, f_s(x)$ be a complete list of the proper, monic divisors (of nonzero degree) of $h(x)$. (If q is not two there are at most 2 local factors of $h(x)$ and $s \leq 4$. If $q = 2$ then there can be arbitrarily many divisors of $h(x)$.)

Given the weight distributions of the three local types I, II, and III, the following method allows us to recursively compute the weight distributions of all cyclic codes with simple orbit structure.

Assume that the following are known for each $i = 1, 2, \ldots, s$,

$$n = \exp(h(x)), \qquad N = |R^*|, \; R = F[x]/(h(x)),$$
$$n_i = \exp(f_i(x)), \qquad N_i = |R_i^*|, \; R_i = F[x]/(f_i(x)),$$
$$W_i = \text{weight of any nonzero element of } R_i^*.$$

Since each $f_i(x)$ divides $h(x)$, by Lemma 2 we know that all elements of R_i^* have the same weight, namely W_i. Now the nonzero nonunits of R can be partitioned into subcodes S_i, where S_i is the set of all elements $f(x) + (h(x))$ in R for which $(f(x), h(x)) = d_i(x)$, where $d_i(x) = h(x)/f_i(x)$. Then we can write

$f(x) = a(x)d_i(x)$, where $(a(x), f_i(x)) = 1$. Then by Lemma 1

$$w_{h(x)}(f(x)) = (n/n_i)w_{f_i(x)}(a(x)) = (n/n_i)W_i.$$

The elements of S_i are in 1–1 correspondence with the elements of R_i^*, so there are N_i such elements. This gives the weight distribution of all nonunit elements of R. Let W be the weight of any unit. All N units have the same weight. Since as is known the total weight of the nonzero code words of an (n, k) code is $nq^{k-1}(q-1)$ we see that

$$W = (nq^{k-1}(q-1) - N_1(n/n_1)W_1 - \cdots - N_s(n/n_s)W_s)/N. \tag{26}$$

(The elements of S_i correspond to the generators of the ideal of $F[x]/(x^n - 1)$ generated by $d_i(x)g(x) + (x^n - 1)$ under the isomorphism between R and C given in Section 1. Since every ideal in C has such a generator, it follows that the set of generators of each ideal in C is a single G-orbit.)

This method is fairly easy to carry out. We list the weight distributions of a few of the different types of cyclic codes of simple orbit structure.

First we list the three local cases:

4.1. $h(x)$ *is of type* I(a, k)

This is an (n, k) code with $n = (q^k - 1)/a$. This code is equidistant.

Table 2

	No. code words	Weights
Units	$q^k - 1$	$q^{k-1}(q-1)/a$
	1	0

4.2. $h(x)$ *is of type* II(a, b)

In this case the code is an (n, k) code with $k = 2$ and $n = p(p-1)/a$.

Table 3

	No. code words	Weights
Units	$p^2 - p$	$(p-1)^2/a$
	$p - 1$	$p(p-1)/a$
	1	0

4.3. $h(x)$ *is of type* III, *i.e.*, $h(x) = (x+1)^3$

In this case $(n, k) = (4, 2)$.

Table 4

	No. code words	Weights
Units	4	2
	2	2
	1	4
	1	0

4.4 $h(x) = h_1(x)h_2(x)$, *where* $h_i(x)$ *is of type* $\mathrm{I}(a_1, k_1)$

We assume further that $(a_1, a_2) = (k_1, k_2) = 1$ and that $h(x)$ is of simple orbit type. For example, $a_1 = q - 1$ and $a_2 = 1$ will suffice by

Theorem 4. In this case $k = k_1 + k_2$ and $n = (q^{k_1} - 1)(q^{k_2} - 1)/(q - 1)$.

Table 5

Weights	No. code words
$(q^{k_2} - 1)q^{k_1 - 1}$	$(q^{k_1} - 1)$
$(q^{k_1} - 1)q^{k_2 - 1}$	$(q^{k_2} - 1)$
$q^{k_1 + k_2 - 1} - q^{k_1 - 1} - q^{k_2 - 1}$	$(q^{k_1} - 1)(q^{k_2} - 1)$
0	1

4.5. $q = 2$ *and* $h(x)$ *is a product of three primitive polynomials* $h_i(x)$ *of pairwise relative prime degrees* k_i, $i = 1, 2, 3$.

In this case $k = k_1 + k_2 + k_3$ and $n = n_1 n_2 n_3$, where $n_i = 2^{k_i} - 1$.

Table 6

No. code words	Weights
n_3	$\frac{1}{2}n_1 n_2(n_3 + 1)$
n_2	$\frac{1}{2}n_1 n_3(n_2 + 1)$
n_1	$\frac{1}{2}n_2 n_3(n_1 + 1)$
$n_2 n_3$	$\frac{1}{2}n_1(n_2 n_3 - 1)$
$n_1 n_2$	$\frac{1}{2}n_3(n_1 n_2 - 1)$
$n_1 n_3$	$\frac{1}{2}n_2(n_1 n_3 - 1)$
$n_1 n_2 n_3$	Use (26).
1	0

Remarks. The approach to cyclic codes pursued in this paper is closely related to and was motivated by the papers of Ecker [6], Boyarinov and Kabatyansky [7] in the theory of cyclic arithmetic codes. The ideas in their papers are in fact more explicit and more precise developments of ideas that go back to the work of Chang and Tsao-Wu [5]. The analogous approach in arithmetic codes is based on

the determination of those integers m for which the group of units $U(m)$ of $Z/(m)$ is equal to the subgroup of $U(m)$ generated by $q + (m)$ and $-1 + (m)$.

References

[1] W.E. Clark, Equidistant cyclic codes over GF(q), Discrete Math. 17 (1977) 139–141.
[2] E.R. Berlekamp, Algebraic Coding Theory (McGraw-Hill, New York., 1968).
[3] B.R. McDonald, Finite Rings with Identity (Marcel Dekker, New York, 1974).
[4] R.W. Gilmer Jr., Finite rings having a cyclic multiplicative group of units, Amer. J. Math. 85 (1963) 447–452.
[5] S.H. Chang and N. Tsao-Wu, On the evaluation of minimum distance of binary arithmetic cyclic codes, IEEE Trans. Inform. Theory IT-15 (1979) 628–631.
[6] A. Ecker, How to compute the minimum distance for cyclic AN-codes over an arbitrary base. I. Elementary methods, Inform. and Control 46 (1980) 219–240.
[7] I.M. Boyarinov and G.A. Kabatyanskii, Arithmetic (n. A) codes over arbitrary base, Sov. Phys. Dokl. 20(4), (1975) 247–264.